

JK Lakshmipat University Jaipur
INSTITUTE OF ENGINEERING AND TECHNOLOGY

End Term Examination, December 2025
B. Tech. (CSE/ECE), Semester VII, 2025-26

Roll No.....

CS1239: Security Engineering

Time: 2 hours

Max. Marks: 30

Instructions to students:

1. Do not write anything other than your roll number on the question paper.
2. Mention all the assumptions for your answers clearly.

Q1.	Malicious Code (Overwrite) New Return Address (Overwrite) (Overwrite)	What is the SET-UID mechanism in Unix systems, and how can it be used by attackers to inject malicious code into the stack? In the adjacent figure, why is the address at which the malicious code is written important? What safety precautions are implemented by operating systems to prevent these attacks?	5.0 (CS1239.2)
Q2.	While using 'Cal' system call on a Unix machine, the system opens a malicious calendar showing dates in the year 2045. What could have gone wrong during the system call, especially if we are using dynamically linked binaries?		5.0 (CS1239.2)
Q3.	What are hallucination guardrails? How can NLI be used for making a hallucination validator? What are the outputs of NLI when it checks the hypothesis with premises, and under what circumstances can we say that the model is not hallucinating? A university campus allows students to use LLM to make assignments. How can fine-tuning the LLM models with a controlled academic corpus help to reduce the hallucination?		5.0 (CS1239.3)
Q. 4	A production LLM chatbot deployed by a fintech platform named FinAssist was red-teamed and subsequently abused by hostile actors. Researchers and attackers used a combination of multimodal prompt injections, system prompt leakage, supply-chain and dependency attacks, and data-exfiltration techniques to extract confidential training data, execute privileged tool calls, and cause the assistant to produce harmful operational instructions. Recommend a questionnaire for the audit by a company that		5.0 (CS1239.4)

	wants to recommend responsible AI for this organization.	
Q. 5	A multinational company, Global Tech Solutions Pvt. Ltd., maintains an operational account at Metro National Bank (MNB). On a Monday morning, the bank's fraud monitoring system detected a series of unusual international wire transfers amounting to USD 2.8 million to accounts in Singapore and the Cayman Islands. These transfers were authenticated using valid PIN-based authorization codes from the company's corporate payment token. Analyze if any weaknesses in key management, HSM configuration, and transaction environment segregation contributed to the success of the fraud. What security measures would you recommend for this large-scale wire transaction?	5.0 (CS1239.5)
Q. 6	QuantumEdge Capital, a hedge fund, suffered major financial losses due to the theft of its proprietary algorithmic trading model (QAlgo-X) by an insider who sold it to a competitor. The stolen algorithm was used to replicate and front-run trades, leading to significant financial and reputational damage. Propose a DeFi-based security framework that could prevent similar fraud in hedge funds, explaining what aspects of cybersecurity would be taken care of by this blockchain.	5.0 CS1239.5

All the best!